КРИПТОВАЛЮТА: ЭЛЕКТРОННАЯ СИСТЕМА РАСЧЕТОВ В ОДНОРАНГОВОЙ СЕТИ

Н. А. Дудин, Аксенов К.А.

ФГАОУ ВПО "Уральский Федеральный Университет имени первого Президента России Б.Н. Ельцина", Екатеринбург, e-mail: megacherepaha@gmail.com

В статье рассматривается функционирование платежной системы на основе криптовалюты. В качестве примера взята криптовалюта Bitcoin. Рассмотрена организация транзакций, обеспечение их безопасности. Рассмотрена возможность для дополнительной эмиссии. Указаны перспективы развития данной криптовалюты.

Ключевые слова: криптовалюта, Bitcoin, peer-to-peer, одноранговые сети, proof-of-work.

CRYPTOCURRENCY: ELECTRONIC SETTLEMENT SYSTEM IN A PEER-TO-PEER

The article discusses the functioning of the payment system based on Cryptocurrency. As an example, taken Cryptocurrency Bitcoin. The organization of transactions, to ensure their safety. The possibility for an additional issue. Shown prospects of this Cryptocurrency.

Keywords: Cryptocurrency, Bitcoin, peer-to-peer, ad hoc networks, proof-of-work.

Введение

В настоящее время система денежных переводов является неотъемлемой частью торгово-рыночных отношений. В структуре денежного перевода всегда присутствует отправитель, получатель и посредник, взимающий за свои услуги определённую плату. Клиенты зависят от третьей стороны, не только при осуществлении денежных переводов, но и в течение всего времени пользования финансовыми услугами. Отказу от услуг третьей стороны, способствует децентрализация системы контроля денежных переводов. На основе этого принципа была создана цифровая валюта получившая название криптовалюты[1]. Таким образом, актуальность темы обусловлена появлением и возможностью широкого распространения финансовой системы, не похожей ни на одну из ныне существующих.

Bitcoin

Учёт и эмиссия криптовалюты основаны на криптографических методах, а функционирование системы происходит в одноранговой компьютерной сети (peer-to-peer). Все ныне существующие криптовалюты, основаны на схожих принципах и протоколах, изначально введенных в валюте bitcoin, поэтому целесообразно будет рассмотреть именно эту валюту.

Рис 1. Блок-схема транзакций

Электронная монета bitcoin определяется как цепь цифровых подписей (математических механизмов, позволяющих кому-либо доказать право собственности). Обладатель может передать монету, создавая цифровую подпись хеша предыдущей транзакции, а также открытого ключа следующего обладателя и добавляя вышеперечисленное в конец монеты (Рис 1) [5, с. 2]. Получатель может проверить подписи для проверки целостности цепи обладателей [5, с. 2].

Котировка Bitcoin

Котировка bitcoin (BTC) основана на доверии к ней, не привязана к какой-либо валюте или другому активу и формируется исключительно балансом спроса и предложения. В свою очередь спрос бывает трех видов:

- спекулятивно-инвесторский (покупка криптовалюты, для ее дальнейшей продажи);
- оплата товаров криптовалютой;
- перевод криптовалюты с одного счета на другой с ничтожно малой комиссией (менее 0.1%).

Bitcoin не имеет органа (центробанка или государства), который бы стремился обеспечить ликвидность на заданном уровне, обязался сам и/или обязывал других принимать оплату в bitcoin-монетах или мог бы искусственно снизить его покупательную способность путём дополнительной эмиссии.

Для получения доверия на рынке, система должна обладать соответствующей степенью безопасности и защищенности переводов.

Безопасность транзакций

Для предотвращения повторного использования одной и той же монеты (double-spending) все транзакции за всё время работы bitcoin хранятся в цепочке блоков. Каждый блок содержит заголовок, включающий хеш предыдущего блока, и список транзакций. Благодаря этому свойству цепочку нельзя подделать, заменив в ней один из блоков, так как хеш блока всегда зависит от хеша предыдущего блока в цепочке. Изменив один из блоков, придется пересоздавать все последующие. Цепочка блоков скачивается целиком каждым клиентом, что делает систему полностью децентрализованной. Данные никак не шифруются, и любой может вручную проследить все транзакции.

Также для защиты от повторного расходования средств, используется метод proof-of-work, основанный на необходимости выполнения запрашивающей стороной ресурсоемкой функции криптографического хеширования (SHA256), результат которой легко и быстро проверяется обслуживающей стороной.

Деятельность, по обслуживанию системы заключающаяся в вычислении этих функций в целях формирования новых блоков, получила название майнинга. Для стимулирования майнинга с каждой транзакции взимается небольшая комиссия, а также вновь выпущенные bitcoin распределяются между майнерами[2].

Эмиссия Bitcoin

Bitcoin предусматривает только одну возможность для дополнительной эмиссии — новые bitcoin начисляются в качестве вознаграждения тому, кто сгенерировал очередной блок, получивший 120 подтверждений. Первоначальная эмиссия составляла 50 BTC за каждый блок, но она уменьшается вдвое каждые 210 000 блоков (примерно раз в 4 года). Таким образом, общее количество bitcoin ограничено значением в 21 млн. BTC.

Перспективы развития

На сегодняшний день bitcoin принимаются в обмен на сетевые услуги и реальные товары. Существует множество площадок по обмену bitcoin на реальные деньги.

Но, несмотря на новизну и непохожесть данной валюты, ей также свойственна непостоянность курса обмена. В начале развития данной финансовой системы, курс составлял 0.003 USD за монету, к июню 2014 года, курс поднялся до 640 USD за монету (Рис 2) [3][4].

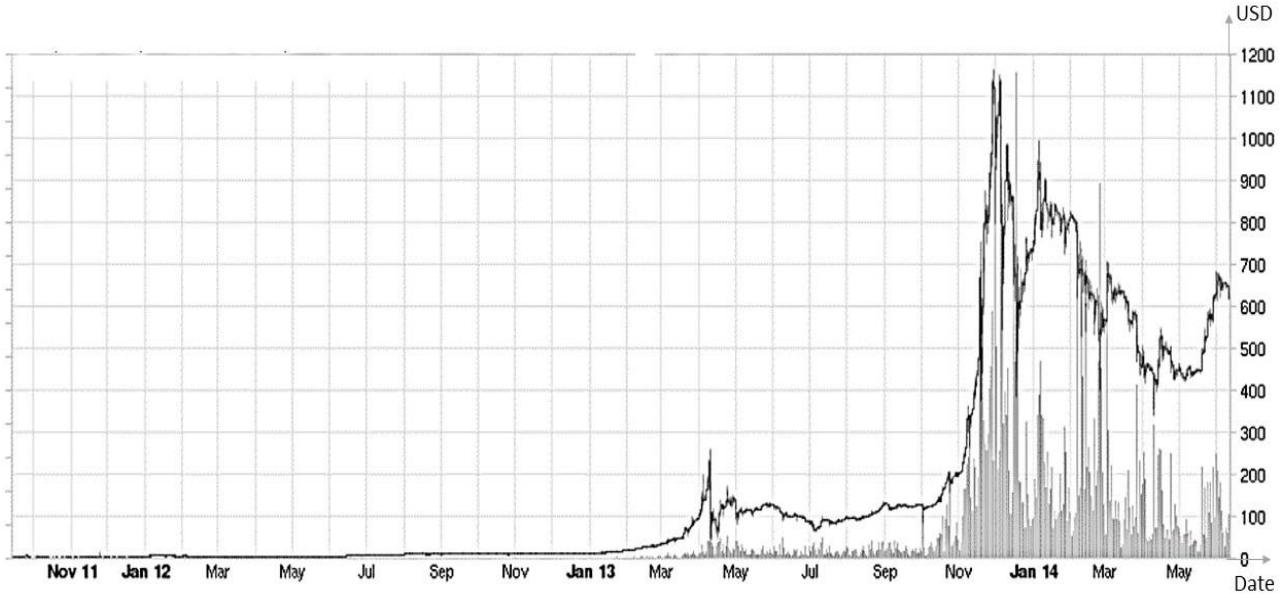

Рис 2. Курс BTC/USD, ось Date информирует о дате, ось USD информирует о стоимость одного BTC в долларах США.

Лимитированность эмиссии bitcoin способствует инфляционной устойчивости, но не гарантирует ее. На данный момент эта устойчивость определяется общим количеством товаров на рынке, которое можно купить за bitcoin.

В заключение можно сказать, что на данный момент bitcoin обладает большим потенциалом, поскольку предлагает беспрецедентные условия денежных отношений. С технической стороны, необходимо отметить инновационность предложенных решений по обеспечению удобства пользования, децентрализации системы контроля денежных переводов и их высокой безопасности, тем не менее, на данный момент, общество относится к криптовалютам скептически, и предпочитает им классические способы денежных переводов. В качестве примера можно привести ситуацию с распространением технологии дальней радиосвязи и беспокойства почтовых служб относительно нарушения своих прав на доставку сообщений. В случае с криптовалютами мы имеем примерно такую же ситуацию - развитие технологий отодвигает в область истории институты, ранее считавшиеся столпами цивилизации.

Список использованной литературы:

1. *Школа Жизни.* [Электронный ресурс]. URL: http://shkolazhizni.ru/archive/0/n-64551/
2. *Bitcoin.* [Электронный ресурс]. URL: https://bitcoin.org/en/
3. *bitstampUSD.* [Электронный ресурс]. URL: http://bbtc.ru/
4. calc.ru [Электронный ресурс]. URL: http://www.calc.ru/kurs-BTC-USD.html
5. *Satoshi Nakamoto.* Bitcoin: A Peer-to-Peer Electronic Cash System, 2009. 9c.